Malware in operating systems

Technology, Information Technology

Malware in Operating Systems: The computer is a set of various components out of which the most important one is the operating system. Operating system can be termed as the backbone of computer. It is the underlying surface over which the entire functions are performed. Operating systems are at direct threat from various kinds of malicious programs which are known as viruses and malwares in the computing world. These are kind of programs designed for specific purpose of destroying data, accessing private records, jamming networks and various other disabilities. The history of malware is an ancient one; a large number of malwares gets enrolled into the world of computer and creates problems of various kinds everyday (Weverka, 2006). Some may target a single computer; others may target networks or servers, while still others aim at banks and official departments. In short, no individual or organization that is being run via online medium is safe from the malware. With broadband technology available to almost every user around the globe, the challenges so faced in regard to the safety of users are more severe now since full time chances of malware entering into the network. Large numbers of operating systems are present in the market, namely Windows by Microsoft, Linux, Android, and Apple Operating System (I. O. S). All of them are vulnerable in one way or another. Every year, we see massive cyber hacking groups launch attacks on official websites, organizations and servers. Many a times, defense organizations become their target as well. Yahoo, Microsoft and other notable websites have become targets of these malwares many a times (Belew & Elad, 2011). Hence, these viruses are not just limited to the individual operating systems, rather, entire cloud and network servers. This malicious content finds their

way in many ways. They can be either penetrated into the system via transfer of files and data, or leaving behind passwords, continuous browsing and extensive online activities are prone to invite the malicious content into the computers (Cooper, 2002). Mostly pop ups and ad on applications lead to entry into the system. The repercussions of all these are highly dangerous and can lead to severe data loss and privacy infringement. Mobile operating systems are equally at threat. For Android, being the major player in this field and so successful at that, challenges for security are also growing in large proportion (Fedler et al 2012). Mac OS and Linux are considered to be slightly safer option in this paradigm. They cannot be termed as hundred percent safe and secure, yet, the probability of catching a worm and getting affected is far more less than that of Microsoft Windows. The numbers of viruses of windows are umpteen; the numbers of other two operating systems mentioned above are relatively smaller in number. The main reason of catching viruses is the process of accepting unauthenticated file and data and allowing remote users access it during conversations. While it is a known fact that the world of internet is full of viruses, the best remedy in this case is a protective operating system and, further, protective browsing. The software design of Linux is comparatively different from the Windows and, hence, makes it hard for hackers and spammers to infiltrate into the respective operating system. Linux, in contrast to Windows, can be termed as program based on secure browsing that invites no or little insurgent elements that are out in the open communication sphere (internet). Microsoft may be relatively user-friendly; yet, this user-friendliness brings about more damages and vulnerabilities on occasions. Linux and Mac OS, in

contrast, ensure safe browsing which might not be the most users-friendly yet secure browsing. The reason for catching less number of viruses can be attributed to the nature of design and the software used. Mac OS are designed in such a way that they ensure safety and are antivirus oriented. The problem with windows is the replication of . exe (executable file) which is often coaxes the users into believing that the file is genuine Windows file (Dvorak et al 2004). Once these files enter in to the system, they spread like fire and make their way to every folder, every drive and every corner of the system. Separation of users into privileged and ordinary users is another factor due to which Linux enjoys considerable safety heaven over Microsoft. In bid to overcome the viruses' factors, Microsoft comes up with official anti-viruses' software that is the company endorsed and ensures protection from various forms of viruses and malwares. They require regular updates and registered member id. Having identified the nature of multiple operating systems, their preferences and priorities, the areas of strength and weaknesses, it can be said that despite the safety functions provided by the operating systems, the users are largely responsible for managing the manner in which their operating system behaves. Safe browsing is the order of the day regardless of any operating system being used. References Belew, S., & Elad, J. (2011). Starting an Online Business All-in-One For Dummies. John Wiley & Sons. Cooper, J. (2002). Special Edition Using Ms-dos 6. 22. Que Publishing. Dvorak, J., Pirillo, C., & Taylor, W. (2004). Online!: The Book. Prentice Hall Professional. Fedler, R., Banse, C., Krauss, C., & Fusenig, V. (2012). Android OS Security risks and Limitations: Practical evaluation. Fraunhofer Research Institution For Applied And Integrated Security.

Weverka, P. (2006). The Everyday Internet All-in-One Desk Reference For Dummies. John Wiley & Sons.